(5)

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 02-041091
(43)Date of publication of application : 09.02.1990

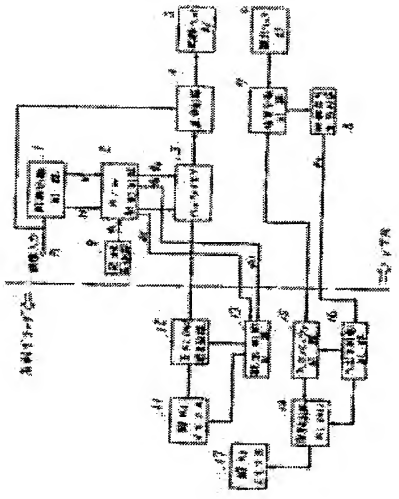
(51)Int.Cl. H04N 7/167

(21)Application number : 63-191782
(22)Date of filing : 29.07.1988

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : HIRASHIMA MASAYOSHI
SATO TOSHICHIKA

(54) SIGNAL RECORDER

(57)Abstract:
PURPOSE: To disable interception even if a reproducing signal is illegally copied by using a specific key at a charged decoder so as to encipher a decoding key and multiplexing it during the horizontal or vertical blanking period.
CONSTITUTION: A key Kt in a Kt memory A11 is enciphered by using a specific key Ki at an enciphering device 12 to generate an enciphering key EKi (Kt) and it is stored in a buffer memory 3. The content of the memory 3 is read for a prescribed period and it is superimposed onto the nH-th TV signal. A mixing circuit 4 eliminates the nH-th scrambled video signal, the EKi (Kt) signal is superimposed and it is recorded on a tape by a recording head section 5. At reproduction, a readout head section 6 reads a recording signal, a decoding circuit 14 uses a key Ki specific to the charged decoder so as to decode the signal, the key Kt is extracted and written in a Kt memory B17. Thus, other charged decoder cannot descramble the signal, then illegal copy is prevented.



(5)

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平2−41091

⑤Int. Cl.⁵	識別記号	庁内整理番号	⑬公開　平成2年(1990)2月9日
H 04 N 7/167		8725−5C	

審査請求　未請求　請求項の数 1　(全6頁)

⑭発明の名称　信号記録装置

⑳特　願　昭63−191782
㉒出　願　昭63(1988)7月29日

⑰発明者　平嶋　正芳　大阪府門真市大字門真1006番地　松下電器産業株式会社内
⑰発明者　佐藤　寿親　大阪府門真市大字門真1006番地　松下電器産業株式会社内
⑰出願人　松下電器産業株式会社　大阪府門真市大字門真1006番地
⑭代理人　弁理士　粟野　重孝　外1名

明　細　書

1、発明の名称

信号記録装置

2、特許請求の範囲

少なくともテレビジョン信号の映像信号と音声信号を記録再生する装置であって、スクランブル化されたテレビジョン信号を復号するデコーダからそのデコーダに固有の鍵Kiを用いて暗号化された解読鍵Ktを読み出すための駆動信号を出力する手段と、前記暗号化された解読鍵Ktをテレビジョン信号中の水平または垂直の帰線期間またはその近傍で記録可能な部分に多重化する手段と、再生信号から前記暗号化された解読鍵Ktを抽出し制御信号と共に前記デコーダへ前記再生信号を供給する手段とを備えたことを特徴とする信号記録装置。

3、発明の詳細な説明

産業上の利用分野

本発明は、有料テレビジョン放送のスクランブル化された映像信号を記録する信号記録装置に関し、特にスクランブル化された信号を再生するための鍵の信号をデコーダから読み出し記録できるようにした信号記録装置に関する。

従来の技術

ＶＴＲ等の録画装置の普及によりテレビジョン放送信号等を録画することが多く行われており、ＣＡＴＶ等の有料放送であっても自由に録画しうる状態になっている。かかるＣＡＴＶの有料放送では信号が暗号化されて放送され、特定のデコーダを有する者のみが復号して視聴することができる。

有料放送のテレビジョン信号を記録する場合には、暗号化(スクランブル)されて送られたテレビジョン信号をそのまま記録するか、一旦復号化(デスクランブル)して通常の映像信号にしてから記録するかのいずれかであった。

発明が解決しようとする課題

ところが、このような暗号化されている有料放送の信号をデスクランブルして記録する場合には、もはや通常の映像信号になってしまっているために自由にテープを再生できることとなり、不正複

写を防げないために有料放送の意味がなくなってしまう。

一方、スクランブル化されているままで記録する場合には、その解読用の鍵（キー）が時間の経過で（たとえば年，月，週，日等の単位で）変更されると解読できなくなる。解読鍵（キー）が変更されなければ、その解読鍵（キー）を保持している有料デコーダであればどの有料デコーダを用いてもテープを再生してデスクランブルして視聴することができることになる。従って、この場合にもスクランブル化されたままのテレビジョン信号を記録したテープを不正複写して盗視聴することができ、有料放送の意味がなくなることになる。

そこで、本発明は、かかる従来の問題点を解消して、不正複写しても盗視聴することができないような信号記録装置を提供することを目的とするものである。

課題を解決するための手段

かかる目的を達成するために、本発明においては、少なくともテレビジョン信号の映像信号と音声信号を記録再生する装置において、スクランブル化されたテレビジョン信号を復号するデコーダからそのデコーダに固有の鍵Ki を用いて暗号化された解読鍵Kt を読み出すための駆動信号を出力する手段と、この暗号化された解読鍵Kt をテレビジョン信号中の水平または垂直の帰線期間またはその近傍で記録可能な部分に多重化する手段と、再生信号から暗号化された解読鍵Kt を抽出し制御信号と共にデコーダへ再生信号を供給する手段とを備えたことを特徴とする。

作用

かかる構成により、各デコーダで固有の鍵Ki を用いて解読鍵Kt を暗号化したものを記録するようにしているため、その鍵Ki を有するデコーダ以外のデコーダでは再生することができるようにすることができ、しかも、このような記録をデコーダと独立して記録装置側で記録信号に多重化して行うことができる。

実施例

本発明の一実施例を第１図に示す。図中、１～９の部分は記録再生装置（たとえばＶＴＲ）であり、１１～１６の部分は暗号解読機能及び暗号化機能を含む有料デコーダの一部を示す。

第１図中、同期分離回路１，記録ヘッド５，再生ヘッド６及び図示していない他の部分は通常のＶＴＲの該当部分と共通の回路等である。また、有料デコーダの図示していない部分たとえばデータ抜取回路，暗号復号回路等は既に実用化されている有料放送（例えばVideo CipherⅡやＢＭＡＣ等）の有料デコーダの当該部分と機能的に同一の回路である。

まず、本発明のシステムの基礎となる暗号化システム全体の概要を第２図，第３図を参照して説明する。ここでは、時間の経過により変化する鍵Kt によって一義的に決まる関数ｆ（Kt）により映像信号及び音声信号をスクランブル化するものとする。鍵Kt を送出側から受信側へ伝送する場合、そのままの形では盗聴されるおそれがあるので、別の鍵Ki で暗号化する。鍵Ki は、端末１台ずつに別々のものを割当てる。このような鍵の重層構造については、たとえば、一松信監修「データ保護と暗号化の研究」第６３頁図１－２７等に記載されている。鍵KtとKi の間に、もう一つ鍵Kt より長い周期で更新される鍵Kxを用いてもよい。このことも同文献に示されている。第３図がその例である。

ここでは、説明を簡単にするために、第２図の場合について説明する。放送の形式として、鍵等の制御信号をデジタル信号で送出できる放送衛星ＢＳ２で採用されている方式を考える。この方式は、音声をデジタル信号で伝送するので、その音声データにＰＮ信号を加算すれば暗号化（スクランブル化）できる。従って、そのＰＮ信号の初期値がすなわち鍵Kt となり、これが判れば復号化（デスクランブル化）できる。この鍵Kt を鍵Ki で暗号化（スクランブル化）して送り、受信側で鍵Ki で復号化すればよい。映像信号については、ラインローテーションによる暗号化（スクランブル化）を行ない、その各ラインでの切断点を上記ＰＮ信号で与えればよく、これについては

公知の技術が使える。

さて、第１図において、有料デコーダでは受信信号（例えばＢＳチューナーのＦＭ検波複合映像出力信号）がそのまま入力される。その信号から、５.７３ＭＨｚの音声搬送波成分と映像信号成分とを分離し、５.７３ＭＨｚのＱＰＳＫ信号を復調して２.０４８Ｍｂｐｓのデジタル信号を得る。ＱＰＳＫ復調回路の出力から音声データ以外の制御信号データを抜取り、その制御信号データから暗号化されている鍵Ｋｔ その他の信号を復号し、復号化出力中の鍵ＫｔをＫｔメモリＡ１１に記憶する。なお、メモリＡ１１の他に鍵Ｋｔ 以外の制御信号を記憶するメモリが別にあることはいうまでもない。

以下の説明ではＫｔ は毎週変化するものとし、端末側では、毎週１回固有の鍵Ｋｉ で、第４図Ｂの信号を解読するものとする。鍵Ｋｔ の配送は例えば月～金の間毎日行ない、第１図のＫｔ メモリＡ１１内を２個のＫｔ 分の容量とし、毎週日曜日の午前零時に切替える等の操作で端末内の鍵Ｋｔ は、その週の鍵Ｋｔ に切替わる。さて、Ｋｔ メモリ１１内にその週の鍵Ｋｔ（以下Kt_1と記す）がメモリされているものとする。一方、第１図一点鎖線の右側はＶＴＲである。Ｐ１ にスクランブルされた映像信号が入力される。なお、音声については簡単の為、デスクランブル化され、左と右のベースバンド音声信号で記録されるものとする。

この映像信号は、垂直及び水平の同期信号の部分はスクランブル化されず、他の部分はいわゆる公知のラインローテーションによりスクランブル化されているものとする。

端子Ｐ１への入力を同期分離回路１で分離し、Ｈパルスとｖパルスを得る。第５図に示す如く、Ｒ／Ｗ制御回路２へ、記録指示回路９から時刻t_1で、記録指示パルスが供給されると、その後の垂直帰線期間の始めの部分で、Ｒ／Ｗ制御回路２からデコーダの読出制御回路１３へt_1'から始まる読出クロックϕ_5が供給される。一方、読出制御回路１３へは、t_1から制御パルスϕ_2が供給され、ＫｔメモリＡ１１の内容Ｋｔを暗号器１２で固有の鍵Ｋｉ を用いて暗号化して暗号化鍵信号ＥＫｉ（Ｋｔ）を作る。t_1'から暗号器１２内のＥＫｉ（Ｋｔ）を読み出しバッファメモリ３へ記憶する。バッファメモリ３の内容をt_2～t_5間にクロックϕ_4で読み出し、第６図に示す如くテレビジョン信号の第２２Ｈ目に重畳する。混合回路４では、ラインローテーションによりスクランブル化された第２２Ｈ目の映像信号を除去し、第４図のＢのＥＫｉ（Ｋｔ）信号を重畳する。これを記録ヘッド部５によりテープに記録する。テープの高域特性が悪ければ、２８８ビットを２Ｈに分けて記録しても支障はない。

他のスクランブル内容に関する信号は、垂直帰線期間（ＶＢＩ）の例えば第２０Ｈ目（又は第２０Ｈ目と第２１Ｈ目の合計で２８８ビット）に２８８ビット、第６図の如く重畳されているものとする。この結果、ＶＴＲのテープには、ϕ_5 の如くt_2～t_3に第４図Ｂの信号を含んだ形で、即ちϕ_0にt_2～t_3 の部分を追加した形で記録される。

次に、記録信号ϕ_5を再生する場合を説明する。読出ヘッド部６でテープから記録信号ϕ_5 を読み出し、信号分離回路７へ伝える。信号分離回路７で第６図の信号中のヘッダ（第４図のＡ，Ｂのヘッダ部）を検出し、制御信号形成回路８で制御信号ϕ_6 を形成し、このϕ_6 を有料デコーダの入出力制御部１６へ供給する。制御部１６からＫｉ（Ｋｔ）デコーダ１４と、入力バッファメモリ１５へクロックを送る。即ち、入力バッファメモリ１５のメモリへ第６図のt_2～t_3からの２８８ビット（第４図Ａに相当）を書込み、続いて、デコーダ１４へ入力バッファメモリ１５の内容を転送し、その有料デコーダに固有の鍵Ｋｉ で解読して、鍵Ｋｔ を取り出し、ＫｔメモリＢ１７へ書込む。

ＶＴＲ出力を有料デコーダに入力する場合、有料デコーダに切替スイッチを設けておき、そのスイッチの切替えによりＫｔ メモリＡ１１の中の鍵Ｋｔ を使うかＫｔメモリＢ１７の中の鍵Ｋｔを使うかを切替える。従って、ＶＴＲの再生出力をデスクランブル化する場合は、Ｋｔメモリ Ｂ１７ の中鍵Ｋｔ 即ち、ＶＴＲテープに記録されている信号

をスクランブル化するために用いた暗号鍵Ｋｔを用いるので、デスクランブル化できる。これは、記録する時に用いた有料デコーダによってのみ可能となる。

なお、送られてくる鍵Ｋｔが変更される迄の間は、他の有料デコーダで記録したスクランブル済の信号を別の有料デコーダで再生することは、有料デコーダの内部結線を変更すれば可能であるが、有料デコーダ側でＫｔメモリＡ１１，Ｋｔメモリ１７、その切替部分をパッケージ化してモールドする等の方法でその結線変更を不可能にすれば防止できる。

以上の説明は、鍵の重層構造が第２図の如く２層の場合であるが、第３図の如く３層であってもよい。３層の場合、鍵Ｋｔでなく鍵Ｋｘを鍵Ｋｉで暗号化して記録し、再生し、第１図のＫｔメモリＡ１１とＫｔメモリＢ１７には鍵Ｋｘを記憶させる。

発明の効果

このように、本発明によれば、時間と共に変更される鍵の更新周期を短かくしておけば、一つの有料デコーダを用いて記録したスクランブル化された信号は他の有料デコーダではデスクランブル化できないので、不法な複写を防止できる。

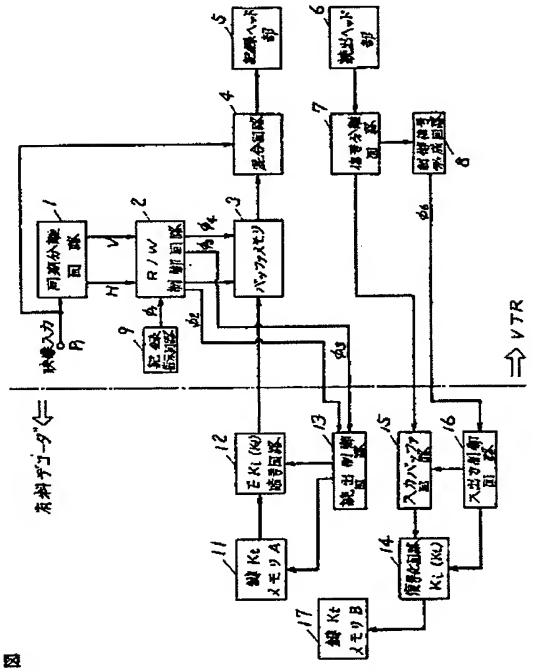
また、有料デコーダの内部構造で物理的に保護すれば、鍵が変化する前でも、他の有料デコーダを用いて記録したスクランブル化された信号をデスクランブル化することはできない。何ぜならば、再生して得られる信号から鍵Ｋｉを用いて解読しても鍵Ｋｔが得られず、一方、有料デコーダで構造的に再生時は再生出力から得られた鍵のみを使えるように構成しておき、その構造を外部より変更できないようにしておくことができるからである。

４、図面の簡単な説明

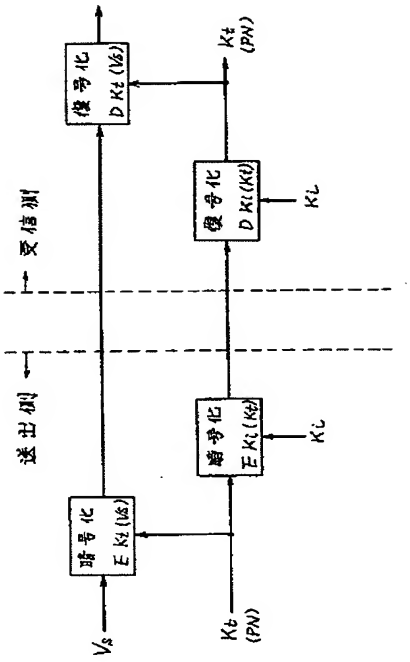
第１図は本発明の一実施例における信号記録装置のブロック図、第２図，第３図はその暗号化，復号化の原理を示すブロック図、第４図，第５図，第６図はその動作を示す波形図である。

１……同期分離回路、２……Ｒ／Ｗ制御回路、３……バッファメモリ、４……混合回路、５……記録ヘッド部、６……読出ヘッド部、７……信号分離回路、８……制御信号形成回路、９……記録指示回路、１１……Ｋｔメモリ Ａ、１２……暗号器、１３……読出制御回路、１４……デコード回路、１５……入力バッファメモリ、１６……入出力制御回路、１７……Ｋｔメモリ Ｂ。

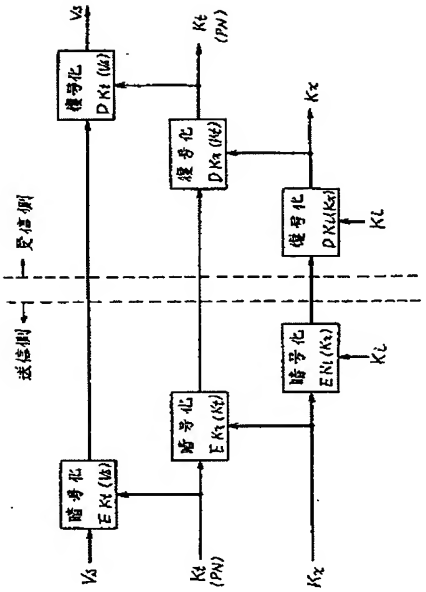
代理人の氏名　弁理士　栗　野　重　孝　ほか１名



第１図

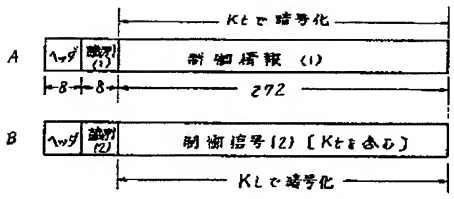


第 2 図

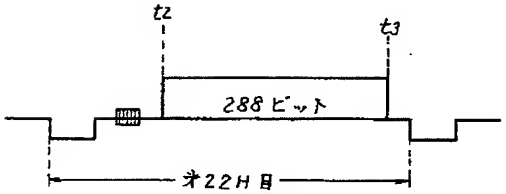


第 3 図

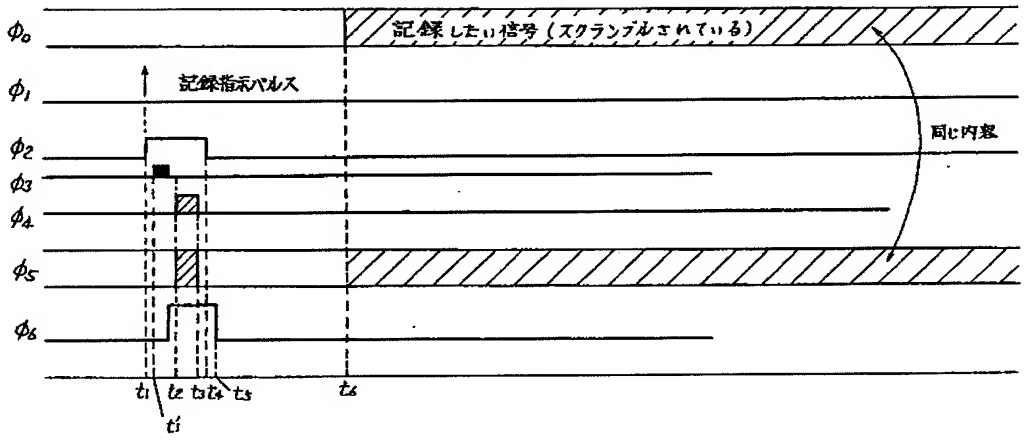
第 4 図



第 6 図



第 5 図


ϕ_0
ϕ_1
ϕ_2
ϕ_3
ϕ_4
ϕ_5
ϕ_6
記録したい信号（スクランブルされている）
記録指示パルス
同じ内容
t_1
t_2
t_3
t_4
t_5
t_6
t_i